Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and

systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues, and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

(FY 2010) PIA: System Identification

Program or System Name:	OM>FSC>HCPS
OMB Unique System / Application / Program Identifier (AKA: UPID #):	N/A
Description of System / Application / Program:	HCPS provides an automated claims processing system from receipt of medical claim documents through claims payment including the appropriate accounting transactions.
Facility Name:	Financial Services Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Cathy Brean	512-460-5175	cathy.brean@va.gov
Information Security Officer:	Krystal Johle	512-460-5043	krystal.johle@va.gov
Chief Information Officer:	Larry Sherman	512-460-5300	Larry.Sherman@va.gov
Person Completing Document:	Tom Rielly	512-460-5108	Thomas.Rielly@va.gov
Other Titles:	Terry Riffell	512-460-5100	terry.riffel@va.gov

Other Titles:	N/A
Other Titles:	N/A
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	10/2008
Date Approval To Operate Expires:	Nov-09

What specific legal authorities authorize this program or system:	Title 38 United States Code (U.S.C) 1703 & 38 CFR 17.52 – 17.56. 38 U.S.C. 1728 & 38 CFR 17.120 – 17.132. Title 18 Section 4006.
What is the expected number of individuals that will have their PII stored in this system:	Potential number of unique patients is 900,000 with continued expected growth.
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	6 Years
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	Yes
Date of Report (MM/YYYY):	11/2009

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☐ Have any changes been made to the system since the last PIA?
- ☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Does this system/application/program collect, store or disseminate PII/PHI data?

☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?	Yes
if the answer above is no, please skip to row 16.	
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	13VA047
2. Name of the System of Records:	Individuals Submitting Invoices/Vouchers for Payment
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://www.rms.oit.va.gov/SOR_Records/13VA047.asp
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	Yes
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	No
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper	Benefits	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	N/A	N/A		
Service Information	Electronic/File Transfer	Benefits	Written	Written
Medical Information	Paper	Benefits	Written	Written
Criminal Record Information	Electronic/File Transfer	Benefits	Written	Written
Guardian Information	Paper	Benefits	Written	Written
Education Information	N/A	N/A		
Benefit Information	Electronic/File Transfer	Benefits	Written	Written
Other (Explain)	N/A	N/A		

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments

Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	Name, address, SSN, ICN, DOB. Information is provided by the healthcare provider to process medical payments. The personal information (SSN, ICN, DOB) is needed to determine if the claimant is actually a Veteran and is elegible. In addition, name and anddress information will be colleced as the Veteran will be notified of the status of their claim by mail.
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	FSC will collect information on the Veteran service related condition, disabilities. These are used during the medical review of the claim.

Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	Medical information is provided by the healthcare provider to FSC to process medical claims. The medical information (medical reports) are provided as supporting documents to allow FSC to determine if the Veteran service related condition, disabilities are associated to cause of the emergency care
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	The FSC will check to see if the Veteran is a fugitive felon during the claims eligibility screening process
Guardian Information	Yes	VA Files / Databases (Identify file)	Voluntary	Name, Address, Phone Number for purpose of emergency contact
Education Information	No			
Benefit Information	No	VA Files / Databases (Identify file)	Mandatory	Vocational rehab information is captured only to determine if the medical claim is eligible.
Other (Explain) Other (Explain) Other (Explain)				

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VISN and Station Level	Yes	Claims processing information for appropriate payment/denial	Both PII & PHI	We have both a MOU and a DTA on file.
Other Veteran Organization	No	No	N/A	N/A	N/A
Other Federal Government Agency	DIHS	Yes	Claim status and disposition.	N/A	Contractual
State Government Agency	No	No	N/A	N/A	N/A
Local Government Agency	No	No	N/A	N/A	N/A
Research Entity	No	No	N/A	N/A	N/A
Other Project / System	No	No	N/A	N/A	N/A
Other Project / System	No	No	N/A	N/A	N/A
Other Project / System	No	No	N/A		N/A

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	HCPS does not gather information from another system.
Per responses in Tab 4, does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	☐ Through a Written Request ☐ Submitted in Person ☐ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?	No

if yes, please check all that apply:	☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)
Describe process for authorizing access to this data.	
Answer: Access is documented on VA Form 9957 and is approved by the supervisor, IT security staff. Only users that have a documented "need to know" have access to the database. IT support user access to database is limited to either production or development database based on their job responsibilities. All system related documents and source codes are stored in version controlled storage database. Any change to the source code is controlled through the change control process and approved by change control board. All users of HCPS go through privacy awareness and cyber security training annually.	

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: FSC will only extract the necessary information from source systems to process the required eligibility data to process and adjudicate medical claims .

How is data checked for completeness?

Answer: Automated adjudication using PLEXIS software.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Data is refreshed monthly from data sharing sources.

How is new data verified for relevance, authenticity and accuracy?

Answer: Authoritative source providers are responsible for the relevance, authenticity and accuracy of data provided..

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer: Records are retained on tape and electronic media for 6 years and 3 months as required by GRS 6, Item 1a.

Explain why the information is needed for the indicated retention period?

Answer: Governed by General Accounting Office Regulations which require retention for records created prior to July 2,1975: 10 years and 3 months after the period of the account; records created on and after July 2, 1975: 6 years and 3 months after the period of the account.

What are the procedures for eliminating data at the end of the retention period?

Answer: We have developed a file plan for the service who is responsible to maintain these records. The file plan identifies where the data is located electronically and the NARA approved GRS are identified. We are working with the IT Staff to develop automated destruction methods of media at the appropriate time based on identified published NARA and VA instructions. Hard copies are destroyed 45 days after receipt and scanned copy becomes the record copy.

Where are these procedures documented?

Answer: System Desk Procedures and VA Directive 6300

How are data retention procedures enforced?

Answer: The FSC will conduct daily checks to ensure documents are being purged (placed in locked shred bins). Scanning supervisor monitors and enforces the retention standards.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13? No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
If 'No' to any of the 3 questions above, please describe why: Answer:	
Is adequate physical security in place to protect against unauthorized access?	Yes
If 'No' please describe why: Answer:	
Explain how the project meets IT security requirements and procedures required by federal law. Answer: HCPS follows all the VA mandated IT security requirements and procedures required by federal law. HCPS servers reside in an access restricted secure location protected by physical access restrictions and environmental protection control measures. User access to the database is limited to as needed basis. The database is further protected by soft wares such as Intrusion Prevention and Detection System, Network Scanner and Patch Management, and Firewall. Further, HCPS is protected by administrative controls such as Security Plans, Rules of Behavior, and Procedures for establishing user accounts	

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- ☐ Air Conditioning Failure
- ☐ Chemical/Biological Contamination
- ☐ Blackmail
- ☐ Bomb Threats
- ☐ Cold/Frost/Snow
- ☐ Communications Loss
- ☑ Computer Intrusion
- ☐ Data Destruction
- ☐ Data Disclosure
- ☑ Data Integrity Loss
- ☐ Denial of Service Attacks
- ☐ Earthquakes
- ☑ Eavesdropping/Interception
- ☑ Fire (False Alarm, Major, and Minor)
- ☑ Flooding/Water Damage
- ☐ Hardware Failure
- ☑ Malicious Code
- ☐ Computer Misuse
- ☐ Power Loss
- ☑ Sabotage/Terrorism
- ☑ Storms/Hurricanes
- ☐ Substance Abuse
- ☐ Theft of Assets
- ☐ Theft of Data
- ☐ Vandalism/Rioting
- ☐ Errors (Configuration and Data Entry)
- ☐ Burglary/Break In/Robbery
- ☐ Identity Theft
- ☑ Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- ☑ Risk Management
- ☑ Access Control
- ☑ Awareness and Training
- ☑ Contingency Planning
- ☑ Physical and Environmental Protection
- ☑ Personnel Security
- ☑ Certification and Accreditation Security Assessments
- ☑ Audit and Accountability
- ☑ Configuration Management
- ☑ Identification and Authentication
- ☑ Incident Response
- ☐ Media Protection

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.
Answer: Collection methods and sources, security controls, and privacy notice.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☐	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☑	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System
Veterans Assistance Discharge System (VADS)
LGY Processing
Loan Service and Claims
LGY Home Loans
Search Participant Profile (SPP)
Control of Veterans Records (COVERS)
SHARE
Modern Awards Process Development (MAP-D)
Rating Board Automation 2000 (RBA2000)
State of Case/Supplemental (SOC/SSOC)
Awards
Financial and Accounting System (FAS)
Eligibility Verification Report (EVR)
Automated Medical Information System (AMIS)290
Web Automated Reference Material System (WARMS)
Automated Standardized Performace Elements Nationwide (ASPEN)
Inquiry Routing Information System (IRIS)
National Silent Monitoring (NSM)
Web Service Medical Records (WebSMR)
Systematic Technical Accuracy Review (STAR)
Fiduciary STAR Case Review
Veterans Exam Request Info System (VERIS)
Web Automated Folder Processing System (WAFPS)
Courseware Delivery System (CDS)
Electronic Performance Support System (EPSS)
Veterans Service Representative (VSR) Advisor
Loan Guaranty Training Website
C&P Training Website
Education Training Website
VR&E Training Website
VA Reserve Educational Assistance Program
Web Automated Verification of Enrollment
Right Now Web
VA Online Certification of Enrollment (VA-ONCE
Automated Folder Processing System (AFPS)
Personal Computer Generated Letters (PCGL)
Personnel Information Exchange System (PIES)
Rating Board Automation 2000 (RBA2000)
SHARE
State Benefits Reference System
Training and Performance Support System (TPSS)
Veterans Appeals Control and Locator System (VACOLS)
Veterans On-Line Applications (VONAPP)
Automated Medical Information Exchange II (AIME II)
Committee on Waivers and Compromises (COWC)
Common Security User Manager (CSUM)
Compensation and Pension (C&P) Record Interchange (CAPRI)
Control of Veterans Records (COVERS)
Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
Fiduciary Beneficiary System (FBS)
Hearing Officer Letters and Reports System (HOLAR)
Inforce
Awards
Actuarial
Insurance Self Service
Insurance Unclaimed Liabilities
Insurance Online
Appraisal System
Web Electronic Lender Identification
CONDO PUD Builder
Centralized Property Tracking System
Electronic Appraisal System
Web LGY
Access Manager
SAHSHA
VBA Data Warehouse
Distribution of Operational Resources (DOOR)
Enterprise Wireless Messaging System (Blackberry)
VBA Enterprise Messaging System
LGY Centralized Fax System
Review of Quality (ROQ)
Automated Sales Reporting (ASR)
Electronic Card System (ECS)
Electronic Payroll Deduction (EPD)
Financial Management Information System (FMI)
Purchase Order Management System (POMS)
Veterans Canteen Web
Inventory Management System (IMS)
Synquest
RAI/MDS
ASSISTS
MUSE
Bbraun (CP Hemo)
VIC
BCMA Contingency Machines
Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

	Name		Description	Comments
			Is PII collected by this min or application?	
Minor app #1			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
			Is PII collected by this min or application?	
Minor app #2			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
			Is PII collected by this min or application?	
Minor app #3			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

Baker System

Dental Records Manager

Sidexis

Priv Plus

Mental Health Asisstant

Telecare Record Manager

Omnicell

Powerscribe Dictation System

EndoSoft

Compensation and Pension (C&P)

Montgomery GI Bill

Vocational Rehabilitation & Employment (VR&E) CH 31

Post Vietnam Era educational Program (VEAP) CH 32

Spinal Bifida Program Ch 18

C&P Payment System

Survivors and Dependents Education Assistance CH 35

Reinstatement Entitelment Program for Survivors (REAPS)

Educational Assistance for Members of the Selected Reserve Program CH 1606

Reserve Educational Assistance Program CH 1607

Compensation & Pension Training Website

Web-Enabled Approval Management System (WEAMS)

FOCAS

Work Study Management System (WSMS)

Benefits Delivery Network (BDN)

Personnel and Accounting Integrated Data and Fee Basis (PAID)

Personnel Information Exchange System (PIES)

Rating Board Automation 2000 (RBA2000)

SHARE

Service Member Records Tracking System

Veterans Assistance Discharge System (VADS)

VBA Training Academy

Veterans Service Network (VETSNET)

Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

BIRLS

Centralized Accounts Receivable System (CARS)

Compensation & Pension (C&P)

Corporate Database

Control of Veterans Records (COVERS)

Data Warehouse

INS - BIRLS

Mobilization

Master Veterans Record (MVR

BDN Payment History

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT	GEN. MED. REC. - I/O	MEDICINE
CLINICAL CASE REGISTRIES	GEN. MED. REC. - VITALS	MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHEVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING	IFCAP	NOIS
DENTAL	IMAGING	NURSING SERVICE
DIETETICS	INCIDENT REPORTING	OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

	Name		Description	Comments
Minor app #1				
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
Minor app #2				
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
Minor app #3				
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

OUTPATIENT PHARMACY

PAID
PATCH MODULE
PATIENT DATA EXCHANGE

PATIENT FEEDBACK

PATIENT REPRESENTATIVE

PCE PATIENT CARE ENCOUNTER
PCE PATIENT/IHS SUBSET

PHARMACY BENEFITS MANAGEMENT
PHARMACY DATA MANAGEMENT
PHARMACY NATIONAL DATABASE
PHARMACY PRESCRIPTION PRACTICE
POLICE & SECURITY

PROBLEM LIST

PROGRESS NOTES

PROSTHETICS
QUALITY ASSURANCE INTEGRATION
QUALITY IMPROVEMENT CHECKLIST
QUASAR

RADIOLOGY/NUCLEAR MEDICINE
RECORD TRACKING

REGISTRATION

RELEASE OF INFORMATION - DSSI

REMOTE ORDER/ENTRY SYSTEM
RPC BROKER

RUN TIME LIBRARY
SAGG
SCHEDULING

SECURITY SUITE UTILITY PACK

SHIFT CHANGE HANDOFF TOOL

SOCIAL WORK

SPINAL CORD DYSFUNCTION
SURGERY
SURVEY GENERATOR

TEXT INTEGRATION UTILITIES

TOOLKIT

UNWINDER

UTILIZATION MANAGEMENT ROLLUP

UTILIZATION REVIEW

VA CERTIFIED COMPONENTS - DSSI

VA FILEMAN

VBECS

VDEF

VENDOR - DOCUMENT STORAGE SYS

VHS&RA ADP TRACKING SYSTEM

VISIT TRACKING
VISTALINK

VISTALINK SECURITY

VISUAL IMPAIRMENT SERVICE TEAM ANRV
VOLUNTARY TIMEKEEPING

VOLUNTARY TIMEKEEPING NATIONAL

WOMEN'S HEALTH

CARE TRACKER

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

	Name		Description		Comments
			Is PII collected by this min or application?		
Minor app #1			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

	Name		Description		Comments
			Is PII collected by this min or application?		
Minor app #2			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

	Name		Description		Comments
			Is PII collected by this min or application?		
Minor app #3			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

(FY 2010) PIA: Final Signatures

Facility Name: Financial Services Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Cathy Brean	512-460-5175	cathy.brean@va.gov
CATHY BREAN Digital Signature Block	Digitally signed by: CATHY BREAN DN: CN = CATHY BREAN O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2009.11.04 13:29:50 -06'00'		
Information Security Officer:	Krystal Johle	512-460-5043	krystal.johle@va.gov
KRYSTAL JOHLE Digital Signature Block	Digitally signed by: KRYSTAL JOHLE DN: CN = KRYSTAL JOHLE O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2009.11.05 08:52:12 -06'00'		
Chief Information Officer:	Larry Sherman	512-460-5300	Larry.Sherman@va.gov
LARRY SHERMAN Digital Signature Block	Digitally signed by: LARRY SHERMAN DN: CN = LARRY SHERMAN O = Department of Veterans Affairs OU = Department of Veterans Affairs, Internal Staff Date: 2009.11.05 08:51:45 -06'00'		
Person Completing Document:	Tom Rielly	512-460-5108	Thomas.Rielly@va.gov
Thomas J Rielly 119407 Digital Signature Block	Digitally signed by: Thomas J Rielly 119407 DN: CN = Thomas J Rielly 119407 O = internal OU = people Date: 2009.11.04 15:01:48 -06'00'		
System / Application / Program Manager:	Terry Riffell	512-460-5100	terry.riffel@va.gov
vafscriffet Digital Signature Block	Digitally signed by: vafscriffet DN: CN = vafscriffet Date: 2009.11.05 08:09:53 -06'00'		

Date of Report:	11/1/2009
OMB Unique Project Identifier	N/A
Project Name	OM>FSC>HCPS